BNL Computer Access Policy

Computer Access Working Group*
February 3, 2004

1. Introduction

Brookhaven National Laboratory's computer network was developed to facilitate sharing of public domain information, primarily fundamental research, by users on the campus and around the world. A small number of these systems contain sensitive but unclassified (SBU) information, some of which is export restricted. This document describes a policy that promotes access to BNL's computer systems, provides ready access to BNL's public domain information by authorized users, and yet maintains appropriate restrictions on systems with SBU information.

Developing BNL's policy is complicated by requirements that control access by foreign nationals to DOE Information Systems. BNL's responsibilities are stated in DOE Orders 205.1, Department of Energy Cyber Security Management Program, DOE Notices 205.2, Foreign National Access to DOE Cyber Systems and DOE Notice 142.1, Unclassified Foreign Visits and Assignments Program. To date, the Notices have been extended by subsequent orders and memoranda. BNL's intention in developing this policy is to comply with the DOE foreign national access requirements by maintaining appropriate controls on computer access by all users, regardless of citizenship.

The policy described in this document applies only to systems that permit users to log into specific accounts on computers. It does not apply to public access to computers through the World Wide Web or other methods. This policy also does not apply to access to Grid computing resources at BNL.

BNL's computer access policy consists of four main components described below. Section 2 contains the requirements for identifying computer systems, including those with SBU information, that require special access restrictions. Section 3 contains requirements for access to BNL computer systems by BNL employees, registered users, and contractors who are authorized to work on the BNL campus. Section 4 describes requirements for remote access to BNL computers by users who will never be physically on-site. Section 5 describes requirements for maintaining accurate records of the users with accounts on BNL computers. The policy described here will be the basis for an SBMS subject area (or areas) on Computer Access.

---

*Eric Blum, Peter Bond, Todd Corsa, James Fung, Gary Gross, Kathleen Hauser, Jerome Lauret, Rachid Nouicer, Martin Purschke, Mark Sakitt, David Siddons, Morris Strongson, Thomas Throwe, Susan White-DePace

2. Critical and Sensitive Computer Identification

Examination of the BNL network has determined that most of the computers at BNL contain only public domain information while a few contain SBU information. Others, such as accelerator control system computers, although containing only unsensitive data, need special access restrictions to guarantee the availability and integrity of their operation. Consequently, it is important to identify the critical and sensitive computer systems and information on the BNL network to ensure that appropriate access restrictions and protective measures are in place for the intended application of each system.

Computers that may require special access restrictions and protective measures are broadly identified as either critical or access controlled. Access controlled systems are further divided into a number of distinct categories. The following categories are defined:

1) Critical System - A system is considered critical when the laboratory or a department cannot complete its mission if the system is unavailable for a period of 24 hours.

2) Access Controlled System- Access to a system must be limited when the information stored on it meets one or more of the following criteria:

   a) Sensitive- Access to sensitive systems is restricted by law. Sensitive data may fall into the following categories as well as others.

      i) Unclassified Controlled Nuclear Information (UCNI)

      ii) Confidential Foreign Government Modified Handling (CFIG/Mod)

      iii) Official Use Only Information (OUO) (see the SBMS subject area on OUO at https://sbms.bnl.gov/standard/38/3817d011.pdf for more information)

   b) Proprietary Data

      Technical data that embodies trade secrets developed at private expense (i.e. design procedures or techniques, chemical composition of materials, or manufacturing methods, processes, or treatments, etc.)

   c) CRADA Information

      A CRADA (Cooperative Research and Development Agreement) is a written agreement between a private company and a government agency to work together on a project.

   d) Privacy Act

      Data related to records maintained on individuals (e.g. Medical Records, Payroll, etc.) Generally, computers holding large personnel databases fall into this category, not individual work stations with a few employee records.

e) Protected Health Information (PHI)

Individually identifiable health information that (a) relates to the past, present, or future physical or mental condition of and individual, (b) can either identify the individual, or there is a reasonable basis to believe the information can identify the individual, and (c) is received or created by or on behalf of a health plan. This information is covered by HIPAA, the Health Insurance Portability and Accountability Act of 1996. Note that employment records held by BNL or BSA in their capacity as employers are not PHI.

All other devices connected to the BNL network that do not fall into one of the categories above are considered to contain only public domain information. They do not require special access restrictions or protective measures. However, access to these systems must be processed in accordance with the procedures specified in the SBMS Unclassified Cyber Security subject area (https://sbms.bnl.gov/standard/2j/2j00t011.htm).

All computers on the BNL network must be registered with the Information Technology Division. In addition to providing the basic identifying information that is required for all computers, system administrators must identify critical or access controlled computers when it is registered for network access. The administrator is also required to indicate the category of access controlled data on the system and to complete a risk assessment questionnaire (and a security plan for Sensitive systems) that describes the protective measures employed. ITD's Cyber Security group uses the results of the questionnaire (and security plan, if required) to perform a risk analysis and make security improvements based on the result of the analysis.

A database of the critical and access controlled computers will be maintained by ITD. The data will be considered Official Use Only and access will be restricted to authorized individuals. Passwords or other measures will be employed to control access. All Web pages, paper copies, and other displays showing this data will be marked Official Use Only.

Other groups share responsibility for identifying sensitive systems/information. The Operations Security Working Group (OPSEC) is responsible for identifying programs with SBU information and the Office of Intellectual Property (OIP) administers CRADAs and Proprietary Research Agreements (PRAs). OPSEC has the particular responsibility to identify programs that must limit foreign national access. OPSEC and OIP will notify Cyber Security of all sensitive programs. Cyber Security will work with the principal investigators (PIs) of the sensitive programs to identify the computers that hold sensitive information. Together with Cyber Security, the sensitive program PIs will work with the computer system administrators to complete the risk questionnaire and perform a risk analysis to ensure that the computers are properly protected. In addition, Cyber security will notify OPSEC of any other site systems that contain sensitive information outside the bounds of the programs that OPSEC identifies, e.g., business sensitive, fiscal records, medical information, etc. Foreign national access restrictions will also be recorded in the registration database. The work flow required to identify, register, and conduct risk assessments of critical and sensitive systems is shown schematically in figure 1.

3. On-Site Computer Access

Accounts on BNL computer systems may be given to active employees listed in the employee database or to active guests or contractors listed in the Guest Information System. Accounts may also be established for retirees listed in the employee database with approval of their former department as described in the SBMS at https://sbms.bnl.gov/standard/2j/2j06d011.htm, Step 5. Most people listed in the employee database or guest information system are already approved for access to the BNL campus; procedures for providing accounts for remote users are discussed in Section 4.

Computer system owners have two options for account management. The owner can ask the system administrator to assign accounts on the system or the owner can ask the ITD Account Management Office to assign accounts. The latter option is normally used for major servers.

Users request accounts on systems managed by the Account Management Office by using the Account Request Form at http://accounts.bnl.gov/. The Account Management Office must verify the user's status in the employee database or Guest Information System before creating the account. An interface to the relevant information in these databases is provided by the Lightweight Directory Access Protocol (LDAP). Web pages will be provided to simplify access to this data, and scripts that query the database to verify the users status will be created for use in automated account creation systems. Users request accounts on systems not managed by the Account Management Office from the administrator of the system; the system administrator must verify the users status using LDAP before creating the account.

The workflow required to create an account is shown in figure 2.

An employee's, contractor's or guest's access to an account must be discontinued when his or her appointment terminates. It is not necessary to delete the user's files as long as the user no longer has access. Methods for preserving the data while denying access vary depending on the operating system of the computer but may include changing the ownership of the directory and files or locking the user's account.

Only active employees, retirees, guests, and contractors may have email accounts at BNL. Before they leave, terminating employees, guests, or contractors may request that the Account Management Office forward their email. (Currently, the SBMS only permits forwarding of terminated employee and retiree email. It will need to be amended to permit forwarding for terminated guests and contractors.) Requests from employees must be approved by their supervisors and requests from guests or contractors must be approved by their BNL sponsor. Mail may be forwarded for a period of, at most, one year from the date of termination.

Additional restrictions are also applied to certain access controlled systems. Accounts may only be created on computers containing SBU information with restricted foreign national access for foreign nationals users whose requests have been reviewed by

Counterintelligence, Export Control, Security, Technology Transfer and finally approved by the Local Approval Authority; accounts for U.S. citizens only need approval from the PI. Accounts on computers with CRADA and PRA information may only be created for users who are approved by the PI.

4. Remote Computer Access

BNL's scientific mission often requires collaboration with people at other institutions. Many of these collaborators may never physically be onsite to work on the BNL campus but will need accounts on BNL computers that they can access remotely. Remote access accounts may only be created for people listed in the Guest Information System as Remote Users.

A person can apply to be a Remote User by using the Access Request Form at https://fsd84.bis.bnl.gov/guest/ and indicating Remote Computer Access as the Purpose of Visit. The applicant must be sponsored by a BNL host (a DOE or BNL employee; note that a sensitive country foreign national cannot be the host of another sensitive country foreign national) and the application must be approved by the sponsor's Department Chairman / Division Manager or the Chairman/Manager's designee. Applicants who are foreign nationals must be processed and approved in accordance with the requirements of SPI 5-09, Unclassified Foreign Visits and Assignments Program prior to receiving an account.

Appendix A indicates that certain delays may be anticipated in applying for remote access. Users should submit their applications early enough so that this does not interfere with the start of their work.

[The following paragraph describes a procedure for creating a temporary account for a user while his or her application is pending. Members of the committee disagreed about whether or not this paragraph should be included. The source of the disagreement comes from the four to six week delays anticipated in approving the IA-473 applications for sensitive country foreign nationals. Some members felt that the delays will be an unacceptable hindrance of their programs. Other members felt that providing access to sensitive country foreign nationals before the approval of their IA-473 will be unacceptable to the DOE. I am including the paragraph for consideration by CSAC and Laboratory management . I expect that CSAC will voice their opinion and that senior management will make the final decision on whether to include it. – Eric Blum, working group organizer]

Considerable time may be required to approve certain foreign nationals' Remote User applications (see Appendix A). Because this lead time may conflict with the legitimate need for a remote user to begin work on a scientific program, the Principal Investigator (PI) or the PI's designee may authorize the creation of a temporary account for the user while the user's application is pending. Temporary accounts may only be granted based on a documented risk assessment for remote access to the information of the program. The risk assessment will be conducted by the program and approved by the PI. Technical assistance in conducting the risk assessment may be provided by the Counter Intelligence

Office, OPSEC, or Cyber Security, as requested by the program. Temporary remote accounts may never be provided on computers with Sensitive information. Access to any temporary account will be terminated if the remote user's application is rejected.

Registered Remote Users may request a computer account using the procedures that are described in section 3. The work flow required to request remote computer access are shown schematically in figure 3.

5. Record Keeping and Account Monitoring

Records must be kept for all accounts that are created on a BNL computer to ensure that accounts are only provided for valid employees, guests, and contractors, including remote users. Each account's record must show the name of the user, the user's life or guest number, the user's status (employee, guest, contractor, remote user), the period for which access is authorized (normally the duration of the user's appointment), who authorized the access, and the user's citizenship.

To simplify record keeping on a critical or sensitive system or on a major server (a computer with accounts for a large number of users and professional system administration), ITD can provide software that will track accounts if that is desired by the system administrator. The system administrator can also keep his or her own records but must be able to provide them for inspection by Cyber Security or other DOE authorities or their contractors. A fraction of the computer systems will by audited annually by cyber security to see that all of the accounts on the system are assigned to valid users.

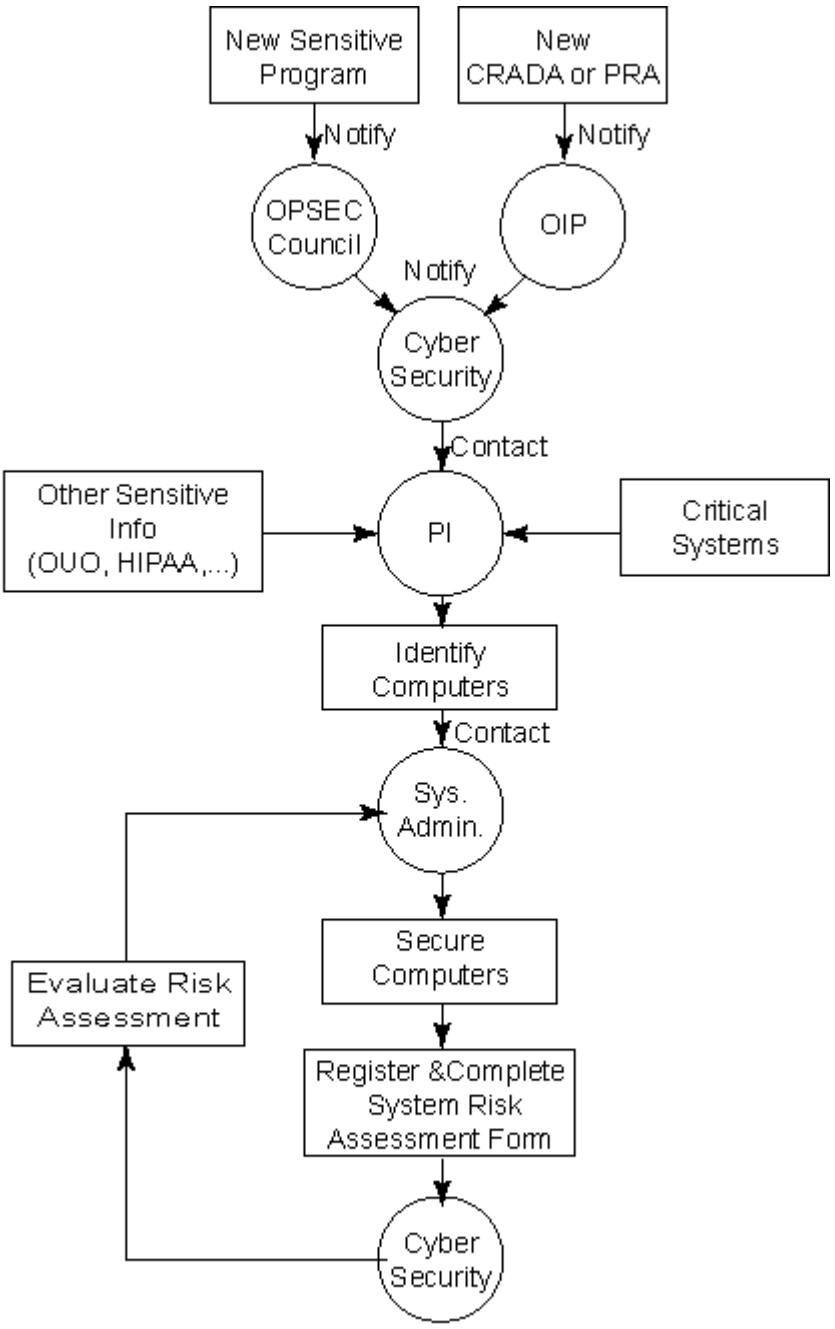

Figure 1. Identification of critical and sensitive systems

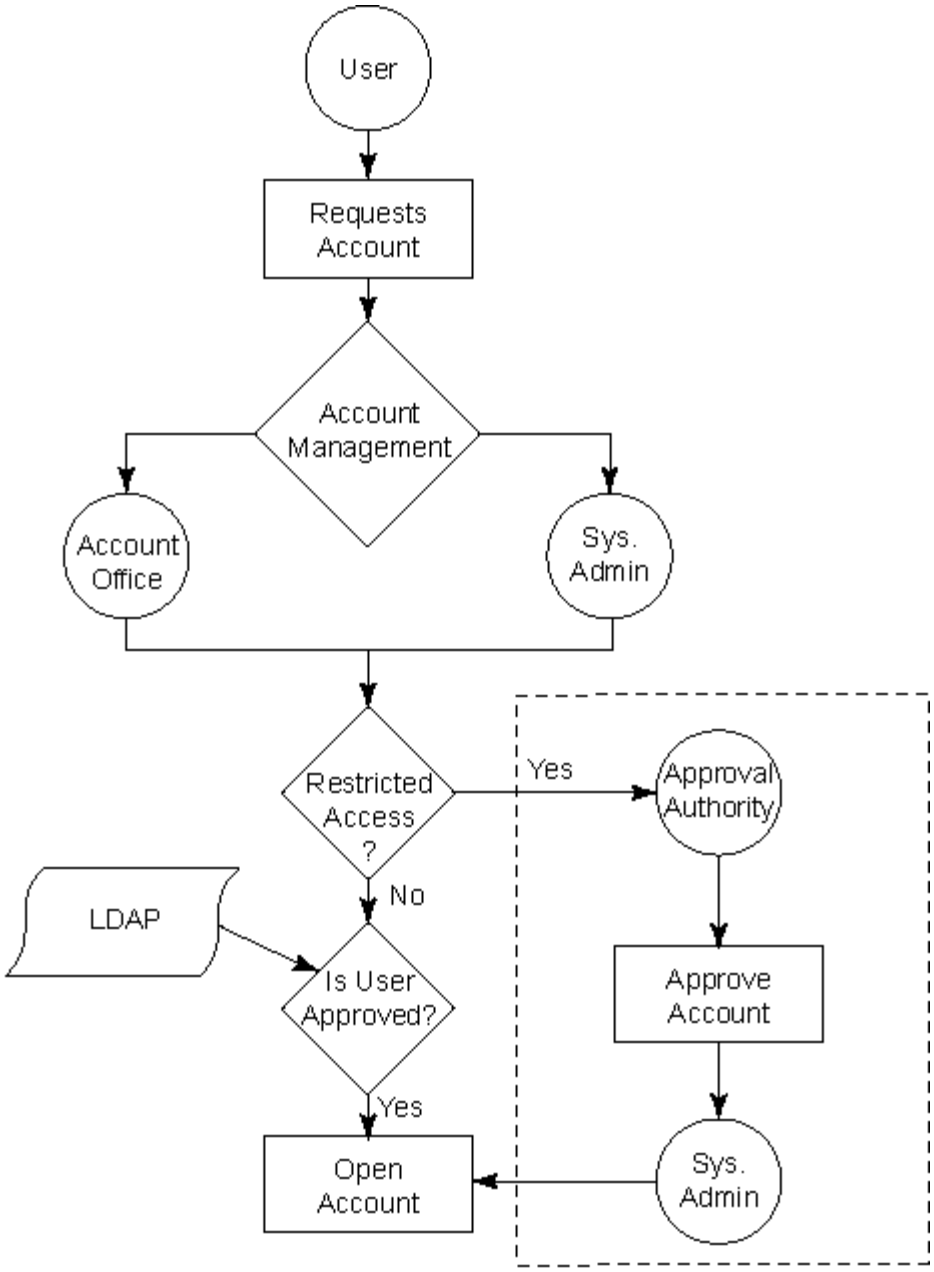

Figure 2. Account creation process

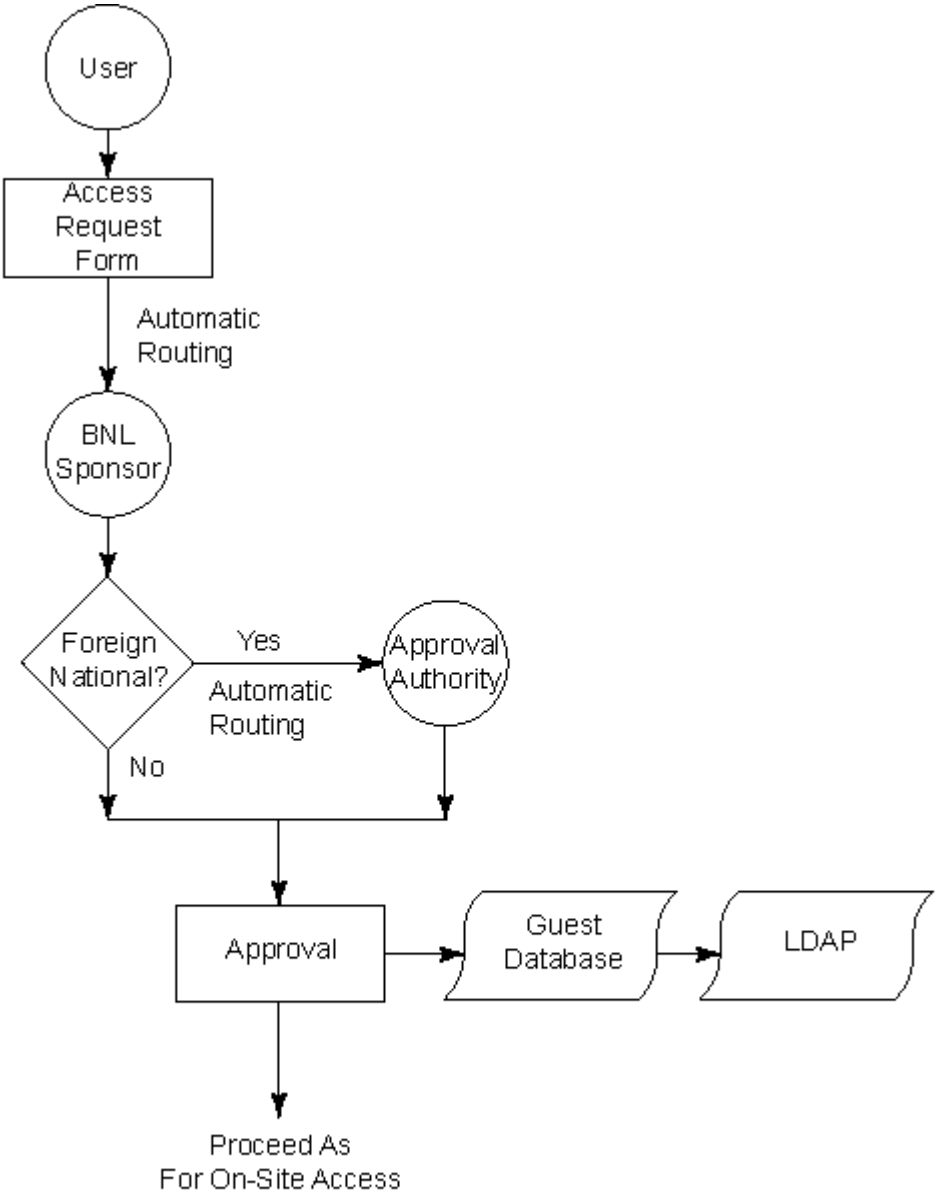

Figure 3. Requesting remote access.

Appendix A. Computer Account Approval Processing Time

The approval lead times noted below are provided only to offer guidance. Most approvals take less time to obtain than indicated, but some approvals take more time.

1. **US Citizens:** The time for approving accounts for US citizens is dependant on the workload of the particular system administrator at any given point of time. The estimated time can range from 1 day to 1 week but is recommended that they be submitted 1 week in advance to allow adequate time for processing.

2. **Non-Sensitive Country Foreign Nationals:** Requests for computer accounts for non-sensitive country foreign nationals, not requesting access to sensitive or critical systems, is 21 days in advance. Account requests for non-sensitive country foreign nationals for access to sensitive or critical systems is a minimum lead-time of 30 days.

3. **Sensitive Country Foreign Nationals:** The minimum lead-time to submit a request for a sensitive country foreign national's computer account is 30 days.

4. **Foreign Nationals from State Sponsors of Terrorism:** Computer account requests from foreign nationals who were born in, are citizens of or work for an affiliation in a country designated by the Department of State as a state sponsor of terrorism, require approval by the Secretary of Energy prior to allowing the issue of an account. At least one hundred twenty (120) days advance notice is necessary for the approval process for these types of account requests.